MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,727	01/03/2001	Rosario Gennaro	RSW920000091US1	3760

43168 7590 04/16/2007
MARCIA L. DOUBET LAW FIRM
PO BOX 422859
KISSIMMEE, FL 34742

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	04/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/753,727
Filing Date: January 03, 2001
Appellant(s): GENNARO, ROSARIO

Marcia L. Doubet
Reg. No. 40,999
For Appellant

EXAMINER'S ANSWER

This is in response to the supplemental appeal brief filed November 20th, 2006 appealing from the Office action mailed February 15, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

GROUNDS OF REJECTION NOT ON REVIEW

The following grounds of rejection have not been withdrawn by the examiner, but they are not under review on appeal because they have not been presented for review in the appellant's brief. The rejection of claim 52 under 35 USC 112 2nd Paragraph, present in the office action mailed 2/15/2007, has not been contested by the appellant as evidenced by the statement made in paragraph 23 of the supplemental appeal brief filed on 7/26/2006.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Patel, Sarvar et al. "An Efficient Discrete Log Pseudo Random Generator", CRYPTO'98, LNCS 1462, 1998, Springer-Verlag Berlin Heidelberg, pp. 304-317

Schneier, Bruce, "Applied Cryptography" 1996, John Wiley and Sons, 2nd Edition, pp. 225, 374-375

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 52 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Although the specification provides antecedent basis for the limitation of top (N-C) bits being set to zero and while the remaining C bits are random, the specification does not provide antecedent basis for (N-C) uppermost **contiguous ones of bits** being set to zero and the lowermost **contiguous ones of bits** being random. As a result, one of ordinary skill in the art would not have been able to determine that the applicant was in possession of the claimed invention. Therefore, claim 52 is rejected for failing to meet the description requirement of 35 USC 112 1st paragraph.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 52 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "effectively-short" in claim 52 is a relative term which renders the claim indefinite. The term "effectively-short" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. One of ordinary skill in the art would not be able to determine how "short" the exponent would need to be in order to be classified as "effectively-short". Therefore, claim 52 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 13-14, 18-19, 21-22, 24-26, 30, 32, 34-35, 37, 39-40, 44, 47, and 49-52 are rejected under 35 U.S.C. 102(b) as being anticipated by Patel et al ("An Efficient Discrete Log Pseudo Random Generator") hereinafter referred to as Patel.

Regarding claim 13, Patel disclosed a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value comprising C random bits (See Patel Page 313 Section 5 Line 10 and section 7.1 s_i wherein C = ω(log n)); means for generating an output sequence comprising N pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12 and section 7.1 x_{i+1}) using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i}$ mod p is one-way, Section 7.1, s as the short exponent, and Page 307 Paragraph 6 Lines 7-8) wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4), means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - ω(log n) bits of x_i and s_i is the leading ω(log n) bits of x_i); and means for using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating (See Patel Section 7.1) while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits (See Patel Section 7.1), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0).

Regarding claim 25, Patel disclosed a programmatic method for efficiently generating pseudo-random bits, comprising the steps of: providing an input value comprising C random bits (See Patel Page 313 Section 5 Line 10 and section 7.1 s_i wherein C = ω(log n)); generating an output sequence comprising N pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12 and section 7.1 x_{i+1}) using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i} \bmod p$ is one-way, Section 7.1 s as the short exponent, and Page 307 Paragraph 6 Lines 7-8) wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4); separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - ω(log n) bits of x_i and s_i is the leading ω(log n) bits of x_i); and using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating (See Patel Section 7.1) while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits (See Patel Section 7.1), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0).

Regarding claim 39, Patel disclosed an encryption system, comprising: means for providing an input value comprising: C random bits (See Patel Page 313 Section 5 Line 10 and section 7.1 s_i wherein C = ω(log n)); means for generating an output sequence comprising N pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12 and section 7.1 x_{i+1}) using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i}$ mod p is one-way, Section 7.1 s as the short exponent, and Page 307 Paragraph 6 Lines 7-8) wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4), means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - ω(log n) bits of x_i and s_i is the leading ω(log n) bits of x_i); and means for using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating (See Patel Section 7.1) while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits (See Patel Section 7.1), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0); and means for using the desired number of generated pseudo-random bits as input to an encryption operation (See Patel Page 305 Lines 15-17).

Regarding claims 14, 26, and 40, Patel disclosed that the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption (See Patel Page 307 Section 2.1).

Regarding claims 18, 30, and 44, Patel disclosed that the C=160 (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and N=1024 (See Patel Page 307 Lines 5-6) (Further see the abstract).

Regarding claims 19, and 32, Patel disclosed that the C is at least 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and N is at least 1024 bits (See Patel Abstract Lines 11-13 wherein n is the number of bits output by the generator prior to bit extraction as disclosed by Patel in Section 6) (Further See Section 7.1).

Regarding claims 21, 34, and 47, Patel disclosed that the (N-C)-bit portion is concatenated to pseudo-random output bits previously generated by the means for generating (See Patel Abstract and Section 7.1).

Regarding claims 22, and 35, Patel disclosed that the (N–C)-bit portion is selected from the N bits of the generated output sequence as a contiguous group of bits (See Patel Section 7.1 Lines 3-4).

Regarding claims 24, and 37, Patel disclosed means for using the desired number of generated pseudo-random output bits as input to an encryption operation (See Patel Page 305 Lines 15-17).

Regarding claims 49, 50, and 51, Patel disclosed that N is greater than or equal to (C*6) (See Patel Abstract wherein C=128 and n=1024).

Regarding claim 52, Patel disclosed a programmatic method for efficiently generating pseudo-random bits, comprising the steps of: providing an N-bit input value in which (N-C) uppermost contiguous ones of the bits are all set to zeros and in which C lowermost contiguous ones of the bits are random (See Patel Page 316 Lines 4-13); generating an output sequence comprising N pseudo-random bits using the provided N-bit input value as an effectively-short, C-bit exponent x of a 1-way function G**x mod P that comprises modular exponentiation modulo a safe N-bit prime number P, wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i} \bmod p$ is one-way, Section 7.1 s as the short exponent, Page 304 Section 1 Lines 3-4, Page 307 Paragraph 6 Lines 7-8, and Page 316 Lines 4-13); separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - ω(log n) bits of x_i and s_i is the leading ω(log n) bits of x_i); creating a new N-bit input value in which the (N-C) uppermost contiguous ones of the bits are all set to zeros and in which the lowermost C contiguous ones of the bits are set to the C-bit portion (See Patel Section 7.1 and 316 Lines 4-13); and using the new N-bit input value as the provided input value for a next iteration of the generation step while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated (See Patel Section 7.1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1-2, 6-7, 9-12, 23, 36, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel as applied to claims 13 and 25 respectively above, and further in view of Schneier ("Applied Cryptography").

Patel disclosed Regarding claims 13, 23, and 36, Patel disclosed a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value comprising C random bits; means for generating an output sequence comprising N pseudo-random bits using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P wherein a base G of the modular exponentiation is a fixed generator value, means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion; and means for using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated (See rejection of claim 13 above), but Patel failed to disclose that this system was implemented in software, and further failed to disclose that the input comprised non-contiguous bits of the previous output. However, Patel did disclose that these pseudo-random bits were for encryption (See Patel Page 305 Lines 15-17).

Schneier teaches that any encryption algorithm can be implemented in software and that doing so helps with flexibility and portability, ease of use, and ease of upgrade (See Schneier Page 225 Paragraph 7 Lines 1-3). Schneier further teaches that software encryption programs are popular (See Schneier Page 225 Paragraph 8 Line 1). Schneier also teaches that in order to reach a maximal period for a pseudo-random bit generator, the feedback bits should be a primitive polynomial mod 2 (See Schneier Page 374 lines 9-20, and further shows an example of this type of feedback (See Schneier Page 375 Figure 16.4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the pseudo-random bit generator of Patel, by implementing the generator in software, and by providing primitive polynomial mod 2 feedback to the generator. This would have been obvious because the ordinary person skilled in the art would have been motivated to improve the portability, ease of use, and ease of upgrade of the generator, and to provide the longest period for the generator to ensure the most produced bits before cycling.

Claims 2, 6-7, 9-10, 12 and 48 are rejected for the same reasons as claim 14, 18-19, 21-22, 24, and 49 above, as applied to claim 1.

(10) Response to Argument

The appellant has presented four different issues.

Issue #1

The appellant argues that the specification does, in fact, support setting the **uppermost contiguous ones of the bits** to zero and leaving the **lowermost contiguous ones of the bits** random. The examiner first points out that the appellants arguments, regarding this issue, are directed towards an input where the uppermost contiguous bits are set to zero and the lowermost contiguous bits are random. As pointed out below, this is not what has been claimed. Also, as pointed out in the rejection, the examiner admits that the specification supports an input where the uppermost contiguous bits are set to zero, while the lowermost contiguous bits are random. It appears that the appellant has misinterpreted the rejection, and as such the appellants arguments appear to be misdirected. As such, the examiner has addressed the arguments as best as possible.

The examiner points out that bits, or *binary digits*, are either ones, or they are zeros. For instance, the bits for the binary representation of the decimal number 14766 are 0011100110101110. In this binary number, 00**111**00110101110, the examiner has bolded and underlined the uppermost contiguous ones of the bits, and is this binary number, 001110011010**111**0, the examiner has bolded and underlined the lowermost contiguous ones the of bits.

As support for the claim language, the appellant has pointed to Page 16, Lines 10-12 as showing support for the claim language:

> *the present invention uses a shorter seed. For purposes of discussion, the seed length is described herein as "C" bits in length, where C< N. All successive inputs also use C-bit values. In other words, the top (N - C) bits of each iteration are set to all zeroes.*

Again, while this supports the scenario where the uppermost (top) N-C bits are set to zero, there is no mention, suggestion, or support for **contiguous ones** being set to zero.

Consider the following scenario with our binary number 0011100110101110, where N=16 and C=14. As supported by the specification, the N-C (2) top bits are set to zero, which results in the same number, **00**11100110101110. However, as claimed, the **<u>uppermost contiguous ones</u>** of the bits would be set to zero, resulting in a different outcome of 00**000**00110101110. As can be seen, what is supported by the specification as pointed out by the appellant, is different from what was added to the claim language.

The appellant further points out that the specification at Page 9 Lines 3-4 supports for each iteration, choosing the next input, from the N produced bits, may either be contiguous bits from the produced bits, or non-contiguous bits. Again, the examiner does not disagree with this statement, but rather points out that this does not provide support for "contiguous **ones** of the bits" being selected. Further, the examiner again does not strongly disagree that "top" and "uppermost" could be used interchangeably, but again this does not provide support for "contiguous **ones** of the bits" being selected.

In summary, the examiner believes that the rejection of claim 52 , for failing to meet the written description requirement of 35 USC 112 1st Paragraph is proper, as the appellant has failed to show support in the specification as filed for "contiguous **ones** of the bits".

Issue #2

The appellant argues, with respect to the prior art rejection of claim 52, that **Patel** does not anticipate each and every limitation of the claim language.

First, the examiner would like to compare the Pseudo-Random Bit Generator (PRBG) of the appellant with the PRBG of Section 5 of Patel.

The appellant's specification as filed, on Page 15 Line 18 – Page 17 Line 9, discloses the iterative generator $x_i = f(x_{i-1})$, which is equivalent to, $x_{i+1} = f(x)$. Appellant's specification further defines f(x) as $f(x) = G\text{^}x \bmod P$. Combining these two equations defines the appellant's generator as:

$$x_{i+1} = g^{x_i} \bmod p$$

Section 5 on Page 313 of Patel gives the following generator:

$$x_{i+1} = g^{x_i} \bmod p$$

The Appellant further teaches use of a short exponent s_i as the input x_i to increase the efficiency of the generator, as can be seen in the specification on Page 18 Lines 12-16, where s_i is a "short" portion of x_i, giving the generator: $x_{i+1} = g^{s_i} \bmod p$

Patel also teaches in Section 7.1 on Page 316 that in order to increase efficiency of the generator, "*we could start with p, g, and x_0* [which is the initial seed] *as earlier but at each stage we define* $x_{i+1} = g^{s_i}$ *wherein s_i = leading* [C] *bits of x_i. This will ensure that at each stage we are using* ***short exponents*** *and hence guarantee a significant speed up.*" This alters the generator of Section 5 of Patel to: $x_{i+1} = g^{s_i} \bmod p$

It is readily apparent from the equations of the two generators, that both the generator of the instant application, and that of Patel, as disclosed in Sections 5 and 7.1, are the same generators, and as such, the appellant's generator was anticipated by Patel. The examiner has further addressed the appellant's specific arguments below.

The appellant argues that with respect to the input to the generator, Patel has not disclosed an N-bit input in which the (N-C) uppermost bits are set to zero and in which the C lowermost bits are random. The appellant points to page 16 Lines 10-12 of the specification as supporting this limitation. This section of the specification reads as follows:

> *For purposes of discussion, the seed length is described herein as "C" bits in length, where C<N. All successive inputs also use C-bit values. In other words, the top (N-C) bits of each iteration are set to all zeroes.*

In the above passage, the applicant has equated the use of a C-bit input, with the use of an N-bit input where the top (uppermost) N-C bits are set to zero. The examiner points out once again that Patel teaches, in Section 7.1 on Page 316, the iterative use of a "C-bit" input, wherein each C-bit input is the leading ω(log n) bits of the previous iteration. As such, Patel has disclosed the equivalent of the claim language, as equated by the applicant. This can further be seen in the following example.

Suppose we have the C-digit number 1234, where C=4. This is the same number as 01234, 001234, 0001234 and 00001234 where N=5, 6, 7, and 8 respectively. Similarly, if we have the C-bit number 1101, where C=4, this is the same number as 01101, 001101, 0001101, and 00001101, where N=5, 6, 7, and 8 respectively. Furthermore, for any number of C-digits, or C-bits, all of the place values greater than the Cth place value of the number are inherently set to zero. Otherwise, the C-digit number 1234, would not have the value 1234, but rather 1001234, or 10001234, etc.

Patel teaches using the leading ω(log n) bits of the previous iteration, as the short exponent input to the generator. Suppose ω(log n) = 4, and the 4 leading bits of the previous iteration are equal to 1101. Again, this input is the same as the inputs 01101, 001101, 0001101, etc. As such, Patel did disclose an N-bit input with N-C uppermost bits set to zero, and C bits which are random (because each iteration of Patel generates random bits).

The claim language, as evidenced by page 16 Lines 10-12 of the application is simply stating that the input is C-bits in length, and thus the place values greater than the Cth bit are zero. The appellant's generator is not actively "setting" these bits to zero, but rather these bits are inherently zero as the input is truly only C-bits in length. This is further evidenced by the appellant's remarks on Paragraph 17, which states that "*Appellant notes that this claim does not specify a 'setting ... ' element.*" As such, the examiner believes that this limitation of claim 52 is properly anticipated by Patel.

The appellant further argues that page 313 does not discuss the generator of Patel, but rather is a proof of security. The examiner agrees with this argument, and notes that the previously cited section of Patel was a typographical error, which has been corrected above to point to the correct Page, 316.

In summary, the examiner believes that Patel does anticipate the claim limitations of having inputs with N-C uppermost bits set to zero and C lowermost bits set to random. As such, the examiner believes the rejection of claim 52 to be proper.

Issue #3

The appellant argues, with respect to claim 13, that Patel does not anticipate each and every limitation of the claim language.

The appellant argues that the "NEW GENERATOR" of Patel section 5 uses an N-bit "large" exponent, and not a C-bit exponent. The examiner agrees with this statement, and points out that the examiner has relied upon the teachings of Patel in Section 7.1 as disclosing the alternative use of a short exponent in order to increase the efficiency of the generator.

The appellant argues that while Patel discloses producing n-c bits per iteration, Patel does not teach using any of the "n-c" bits as input to the next iteration. The examiner first notes that in the above statement the appellant has mischaracterized the teachings of section 7.1. Patel disclosed on Page 316 Lines 5-14, that each iteration of the PRBG generates x_i and that "the output of the generator are the trailing n-[c] bits of x_i". As such, Patel actually discloses producing x_i, which consists of n bits, and outputting n - ω(log n), or N-C, bits as random bits. Patel further disclosed that the leading ω(log n), or C, bits of x_i could be used as a short exponent input s_i for the next iteration. So in fact, Patel did disclose using C-bits of the produced x_i as input to the next iteration.

The appellant argues that Patel teaches drawbacks to using a short exponent, such as a decrease in security, and further teaches other embodiments, such as use of a perfect extender, which could potentially solve the security issues associated with the short exponent. The examiner points out that the generator disclosed in lines 5-14 of Page 316 of Patel, as well as the "perfect extender" version, are alternative embodiments of the "NEW GENERATOR" of Section 5 on Page 313 of Patel. The examiner has neither relied solely upon the generator of section 5, nor has the examiner relied upon the generator using a perfect extender. Instead the examiner has relied upon the generator of section 5 of Patel, modified for efficiency as taught by Patel in Lines 5-14 of Page 316. This is the particular embodiment, which was disclosed by Patel, that anticipates the claim language, as discussed above.

The appellant argues that the claimed invention does not use a "perfect extender". First, the examiner notes that this is not a relevant argument, as the examiner has not relied upon that particular embodiment as anticipating, but rather relied upon the "short exponent" embodiment as anticipating the claim language. Second, the claim language does not indicate that a perfect extender is not, or cannot be used. And finally, as the examiner has shown above, the appellant's generator and the "short exponent" generator are the same iterative generator, using the same mathematical function in the same way to generate the random bits.

The appellant argues that section 5.1 of Patel does not pertain to Patel's generator, but rather to the proof of security of that generator. First, the examiner points out that section 5.1 does pertain to the proof of security of the generator of section 5, and as such does pertain to the generator. Second, the examiner has not relied upon section 5.1 of Patel in showing that Patel did anticipate the claims. As such, the argument is not relevant to the applied rejection.

In Paragraphs 40-41 of the appeal brief, the appellant argues that section 5.1 of Patel shows that the use of short exponents in the generator of section 5 renders the generator not secure. The examiner notes that section 5.1 of Patel is used to prove that the generator of section 5 **is secure** and does not prove that the use of short exponents renders the generator not secure. In fact, Patel goes on to say on Page 314 Lines 13-15, that "*Assuming it is intractable to invert the function g^s mod p where s has* [c] *bits (i.e., short exponent) then the output sequence of our generator is polynomially indistinguishable.*" In other words, Patel proves that as long as the function g^s mod p is a one-way function, which it is assumed to be, then the generator of section 5 of Patel is secure.

In Paragraph 43 of the appeal brief, the appellant states that "if the input value can be recovered when given the output value – according to Patel's Theorem 9 – then the output value is not pseudo-random". The examiner does not see where this is stated anywhere in Patel, and strongly disagrees with this statement. The appellant has made this incorrect statement of "fact", a false premise, in order to come to the conclusion that Patel is not generating pseudo-random bits, which is required by the claim language. First, whether the input can be recovered from the output is not relevant to whether the output is pseudo-random. Instead, it is relevant to whether the pseudo-random bits are secure or not. The examiner notes that the claims do not require that the pseudo-random bits are secure. Second, Patel's Theorem 9 does not state that the input of the generator can be discovered from the output of the generator. As such, the examiner does not believe that these arguments are relevant. Lastly, as shown above, the generators of the appellant and of Patel section 7.1 are the same. So assuming, for arguments sake, that the bits of Patel are not pseudo-random, then neither are the appellant's bits. Furthermore, if the appellant's bits are pseudo-random, then so are the bits of Patel's generator using short exponents.

The appellant further argues that the function of Patel is not 1-way and is not secure. The examiner first notes that the claim language does not require the function to be secure, but rather just 1-way. Again, as shown above, the generators of the appellant and of Patel section 7.1 are the same. So assuming, for arguments sake, that the function of Patel is not one way, then neither is the function of the appellant. Furthermore, if the appellant's function is one way, and secure, then so too is the function of Patel's generator using short exponents. Even further, Patel specifically states that the function is one-way in the first paragraph of section 1 of Patel on Page 304. As such, the examiner believes that the function is one-way.

The appellant argues in Paragraph 44 of the appeal brief that Patel's "NEW GENERATOR" does not a C-bit portion of the generated N-bit output as the input to the next iteration, but rather uses all N-bits of the generated output as the input to the next iteration. The examiner notes that the appellant is referring to the generator of section 5 of Patel, and not to the generator of section 7.1, which the examiner has relied upon. Patel disclosed on Page 316 Lines 5-14, that each iteration of the PRBG generates x_i and that "the output of the generator are the trailing n-[c] bits of x_i". As such, Patel actually discloses producing x_i, which consists of n bits, and outputting n - ω(log n), or N-C, bits as random bits. Patel further disclosed that the leading

ω(log n), or C, bits of x_i could be used as a short exponent input s_i for the next iteration. So in fact, Patel did disclose using C-bits of the produced x_i as input to the next iteration.

The appellant, in Paragraph 45, further falsely states that "Patel admits that he does not know how to make his generator work if only C bits are used as the exponent". Patel makes no such statement, but rather, in section 7.1, states that while the use of short exponent increases the efficiency of the generator, it decreases the security, and as such Patel does not recommend using this generator. This, however, does not take away Patel's anticipation of the generator, or "knowledge of how to get it to work", which is explained in Lines 5-14 of Page 316. Instead, Patel simply discourages the use of the short exponent. In fact, in order for Patel to have determined that the use of the short exponent in the generator would increase efficiency, but decrease security, Patel must have evaluated the generator and thus had possession of the generator and therefore anticipated the generator.

The appellant further argues that Patel has not enabled the generator which uses short exponents on the basis that Patel states that the use of short exponents in the generator lowers the security of the generator and is therefore inapplicable. The examiner points to Patel Page 316 Lines 5-14, wherein the following was disclosed:

> *Let us focus on the mechanics of the generator. We start with a finite field, and a generator g of its multiplicative cyclic group. Let x_0 be a secret seed. Then we define $x_{i+1} = g^{x_i}$ iteratively. The output of the generator are the trailing n − ω (log n) bits of x_i for all i > 0, where n = log p.*
>
> *Although the number of bits generated per iteration is large, each iteration involves a large exponent and this could impact on the speed of the generator. Instead, we could start with p, g, and x_0 as earlier but at each stage we define $x_{i+1} = g^{s_i}$ where s_i = leading ω (log n) bits of x_i. This will ensure that at each stage we are using short exponents and hence guarantee a significant speed up.*

The above section clearly enables one of ordinary skill in the art to make the generator using short exponents. Patel showed which bits to use for the short exponent, and which bits to be output as the random bits. Patel disclosed the formula for the generator, and disclosed how the short exponent was used. As such, the examiner believes that the teachings of Patel are enabling. Further, the appellant has provided no evidence that suggests that one of ordinary skill in the art would be unable to make the generator of Page 316 Lines 5-14.

In summary, the examiner believes that it has been shown that Patel does meet every claim limitation in claim 13, and has done so in an enabling manner. As such, the examiner believes that the rejection was proper.

Issue #4

The appellant argues that a *prima facie* case of obviousness has not been established in view of Patel and Schneier. The appellant relies on the reasoning that not all of the claim limitations have been met by Patel, as argued with respect to claim 13, and that Schneier does not remedy these deficiencies. The examiner has, therefore, relied upon the same reasoning presented for Issue #3 in believing the rejection under 35 USC 103(a) was proper.

To summarize, the examiner has addressed the appellant's arguments:

As per Issue #1, the examiner has addressed the appellant's arguments regarding whether or not there is support for the claim language of claim 52 in the specification. The examiner has shown that the particular wording of the claim language has introduced new matter, which is not supported by the specification.

As per Issue #2, the examiner has addressed the appellant's arguments regarding the prior art rejection of claim 52, and has further shown that the appellant's generator is the same generator disclosed in Patel.

As per Issue #3, and Issue #4, the examiner has addressed the appellant's arguments regarding the prior art rejection of claim 13. The examiner has shown that Patel not only disclosed the claimed bit generator, but further enabled the generator. The examiner further addressed the appellant's remarks with respect to the alleged security, or lack thereof, of Patel's generator, and further pointed out that the claims do not require the generator to be secure.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Matthew Henning

March 29, 2007

Conferees:

Taghi Arani

Eddie Lee

EDDIE C. LEE
SUPERVISORY PATENT EXAMINER